Advisory and Resource Facilitation
National Informatics Centre.
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
IP No 5578
Csg-advisory@nic.in

NIC-CISG/2024-12/588
Dated: 23-12-2024

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Special Advisory for Republic Day (Preventing Web Intrusion Attacks)

Description:

The Republic Day Parade(RDP) and Beating The Retreat Ceremony(BTR)-2025 is schedule on 26 & 29 January 2025 at Kartavya Path and Vijay Chowk in New Delhi respectively. This is very prestigious and sensitive National event, which will attract the attention of malicious cyber threat actors with a view to impact the smooth conduct of the event thus causing harm to prestige of the Nation. The themes/programmes for Republic Day may be weaponized as threat vectors, well before the event as subjects of phishing emails etc. In view of the mentioned cyber threat, please find below:

Measures for prevention of Web intrusion attacks/Web Defacement:

1. SOC Team to be kept on alert to monitor all web facing interface for any suspicious activity.
2. Use latest version of Web server, Database Server, Hypertext Processor (PHP).
3. Apply appropriate updates/patches on the OS and Application software.
4. Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug the vulnerabilities found.
5. Validate and sanitize all user inputs, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
6. Enable and maintain logs of different devices and servers and maintain the same for all the levels.
7. Use Web Application Firewall (WAF), Security Information and Event Management (SIEM) and/or Database Activity Monitoring (DAM) solutions.
8. Search all the websites hosted on the web server or sharing the same DB server, for the malicious web shells or any other artefact.
9. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed. In order to identify Web shells, scan the server with Yara rules.
10. Change database passwords of all the accounts available in the compromised database Server. Also change the passwords/credentials stored in the databases present on the database server.
11. Use an application firewall to control input, output and/or access to the web application.
12. Limit the file types allowed to be uploaded to the web server by using a list of predetermined file types. Define permissions on the directory the files are uploaded into, to prevent attackers from executing the files after upload.

13. Consider using File Integrity Monitoring (FIM) solution on web servers to identify unauthorized changes to files on the server.